REMARKS

Piecemeal prosecution

The applicant objects to the piecemeal prosecution of this application evidence by the most recent official action. An appeal brief has already been filed and the issues raised by the Examiner in the most recent official action could have been raised before the appeal brief was prepared. See MPEP 707.07(g). Piecemeal prosecution is inefficient and is neither in the applicant's nor the USPTO's best interests.

The 35 USC 112 Rejections

Regarding claims 1-7 and 19-21, the Examiner thinks the following claim 1 phrase, concerning what the second-party computer entity does, is unclear:

> "computes first, second and third verification parameters as the product of a second secret with said shared secret, the second element and the first element respectively"

The examiner's interpretation (see lines 3-5 on page 3 of the Action) is wrong. In long-hand, the quoted passage reads as follows:

"computes:

- a first verification parameter as the product of a second secret with said shared secret,

- a second verification parameter as the product of the second secret with the second element,

- a third verification parameter as the product of the second secret with the first element,"

Using the symbols appearing in the description and drawings to represent the quantities concerned:

the first verification parameter	$X = (r).(s_1 Q_{TA2})$;
the second verification parameter	$Y = (r).(Q_{TA2})$;
the third verification parameter	$Z = (r).(P)$

where:

(r)	is the " second secret ".
$(s_1 Q_{TA2})$	is the "shared secret" generated as the product of the first secret (s_1) and the second element (Q_{TA2}).
(Q_{TA2})	is the "second element" – this is an element of a second algebraic group (G_1) and is formed from a public identifier string ("TA2) using a hash function.
(P)	is the "first element" – this is a public element of a first algebraic group (G_1).

The quoted passage of claim 1 would be somewhat clearer if the word "respectively" is re-positioned as follows:

"computes first, second and third verification parameters as the product of a second secret with, respectively, said shared secret, the second element and the first element". As such, claim 1 has been amended to reposition the word "respectively" as indicated. A "long form" version of claim 1 now appears as new claim 29.

Regarding claims 8-11 and 22-24, the examiner thinks the following phrase is unclear because it uses "both" when four items follow:

> "receiving in respect of the second party both an identifier string, and first, second and third verification parameters;"

It should be clear using normal English language construction that "both" refers to 'an identifier string' on the one hand, and 'verification parameters' on the other. In any event the word "both" has been deleted from claim 8 since it is superfluous to the clarity of the claim.

Regarding claims 6-11 and 22-24, the examiner objects to the clarity of:

"carrying out a first check:
p(third verification parameter, computed second element)= p(first element, second verification parameter)
carrying out a second check:
p(first element, first verification parameter)= p(first product, second verification parameter)"

Unfortunately, the examiner does not make it clear why he thinks this phraseology is unclear. The examiner's assertion that nothing follows "first check" or "second check" is obviously incorrect as he goes on to explain the meaning of the following equalities. In any event, the words "to determine that the following equality is satisfied" has been added after first check" and "second check" in the claims.

The 35 USC 101 Rejections

Regarding claims 1-5, the examiner thinks that the elements of the claim 1 merely recite mathematical algorithms. The examiner is mistaken. The invention of claim 1, for example, has clear utility which would be readily recognizable to those skilled in the art.

Claim 1 is for "A method of enabling second party to prove to a third party the existence of an association between the second party and a first party," and in carrying out this method a second-party computer entity:

receives ...

computes ... and

outputs … .

Verification parameters are computed and output – in practical terms this now permits a third party to satisfy themselves that an association exists between the first and second parties. The is a real world problem which the present invention addresses. The inventions of claim 1-5 have the requisite utility to pass muster under 35 USC § 101. See MPEP 2107.

Regarding claims 6-7 the examiner raises essentially the same issue as was raised against claims 1-5.

Claim 1, upon which claim 6 depends, is for "A method of verifying an association between the first and second parties of claim 1" and in carrying out this method a third-party computer entity:

computes…

carries out a first check…. and

carries out a second check.

The examiner says that "Although claim language recite 'the association between the first and second parties being treated as verified if both checks are passed', no practical application (besides mathematical steps/checks) is actually performed at the end, such as an actual process is not claimed". This assertion is incorrect. Claim 6 ends with "the association between the first and second parties being treated as verified if both checks are passed". So the association mentioned in the preamble of claim 1 is proved. Nevertheless, claim 6 has been amended slightly to restate this limitation in more method-like terminology:

"verifying the existence of an the association between the first and second parties only where both checks are passed".

As in the case of claims 1-5, these claims address a real world problem with a real world solution. The claims mass muster under 35 USC § 101. See MPEP 2107.

Regarding claims 8-11, the examiner raises again the same issue. Claim 8 has been amended in a manner similar to claim 6 to restate the last limitation using more method-like terminology.

Regarding claims 22-24, the examiner makes different assertions. The examiner says: "all of the claimed 'means for' can be implemented in computer program or software alone". Oh? Is that so? It is believed that the examiner would soon find a need for a computer to run his program. A program only becomes 'means for' in cooperation with a computer. And claims directed to a programmed computer are patentable in the United States. The rejection is without merit.

The examiner is respectfully requested to place all factual assertions in affidavit form. See 37 CFR 1.104.

The 35 USC 103 Rejections

The examiner has used Gentry 554, Boneh and Gentry 885 in rejecting the claims as being obvious, the primary reference being Gentry 554.

Figure 1 of Gentry 554 gives a general view of the Gentry invention but omits certain details (for example, of the 'intermediate shared secret'). As in the present disclosure, Gentry makes use of pairings (Weil or Tate). Figures 4 and 5 are the detailed embodiments. Since the Figure 5 embodiment is clearly closer to the present claims than that of Figure 4, the applicant will concentrate on the Figure 5 embodiment (the examiner has, however, given references to both embodiments in his arguments against claim 1).

Gentry 554 discloses a Private Key Generator (PKG) that has a secret **s** which it uses to supply two entities A and B with respective secrets $\mathbf{S_A}$ (= $\mathbf{sP_A}$), $\mathbf{S_B}$ (= $\mathbf{sP_B}$) where $\mathbf{P_A}$ and $\mathbf{P_B}$ are public elements formed from the identities of the entities A and B respectively – see [0022] of Gentry.

The two entities A and B can now, without more ado, form a non-interactive shared secret $\mathbf{S_{AB}}$ by using bilinear mapping as is explained at line 14 of Gentry [0022].

The entities A and B also form an interactive shared secret by the exchange of intermediate shared secret components. Thus, for the Figure 5 embodiment, entity A which has a secret **a**, passes **aP** to entity B, whereas entity B, which has a secret **b**, passes **bP** to entity A; **P** is a public element. Both entities can now form **abP**. This is described in [0033] of Gentry.

The entities now go on to form a common symmetric key using at least the interactive shared secret. The formation of the symmetric key seems to be the purpose of the Gentry arrangement, the symmetric key being used to secure communication between the entities.

Differences between Gentry 554 and Claim 1

In the current official action, the examiner's arguments against claim 1 are shorter and clearer, though still incorrect. Considering in turn the three steps carried out by the second-party computer entity of claim 1:

> **"receives a shared secret provided by the first party as the product of a first secret and the second element;"**

The examiner equates the "shared secret" of claim 1 with the interactive shared secret **abP** of Gentry 554 Figure 5. In doing this, it appears the examiner equates the entity A/B of Gentry 554 (it makes no difference which entity) to the second-party computer entity of claim 1. However, in Gentry 554, the

interactive shared secret **abP** is not received as such by either entity A or B from another party:

- Entity A calculates **abP** by multiplying its secret **a** by the 'second intermediate shared secret' **bP** it receives from entity B;
- Entity B calculates **abP** by multiplying its secret **b** by the 'first intermediate shared secret' **aP** it receives from entity A;

The interactive shared secret **abP** of Gentry 554, Figure 5 therefore does not equate to the "shared secret" of claim 1; similarly, the interactive shared secret $\mathbf{g^{ab}}$ of Gentry 554, Figure 4 does not equate to the "shared secret" of claim 1. The examiner may be confused – thus, at line 9, page 7 of the Official Action the examiner refers to "shared secret elements/components" as if this was the same as the shared secret itself, which is not the case.

It might, however, be argued that the first/second intermediate shared secret of Gentry 554 equates to the "shared secret" of claim 1.

> **"computes first, second and third verification parameters as the product of a second secret with said shared secret, the second element and the first element respectively;"**

The examiner has already indicated (lines 3-5, page 2 of the Official Action) that he is reading this passage incorrectly. See applicant's comments above regarding the examiner's misreading of this limitation. Since it suffices to point out to the examiner that his interpretation is incorrect and that claim 1 has been clarified appropriately in response to the 35 USC § 112 rejection, there is little point in spending a lot of time on the examiner's reading of the mischaracterized passage of claim 1 on Gentry 554. However, applicant notes that:

• the examiner's equating of the first verification parameter to **abP** necessarily means that **abP** is not the 'shared' secret of claim 1 as just argued by the examiner for the preceding step (but it is consistent with the intermediated shared secret **aP** being the 'shared secret').

• if the second verification parameter is **b**, then according to the examiner's argument, the 'second element' of claim 1 must be the same as the 'second secret'.

> **"outputs the first, second and third verification parameters for use by the third party in proving the association between the first and second parties."**

The examiner equates this to the "outputting of the interactive shared secret, second and first intermediate shared secret components" (line 18, page 7 of the Official Action); that is to the outputting of **abP**, **bP**, **aP**. This is, with all due respect, absurd because:

the examiner has the second verification parameter being different things in this step and the preceding one (i.e. **bP** here and **b** in the previous step); and

the first, second and third verification parameters are all output by the same entity in claim 1 (the second-party computer entity) whereas, the 'interactive shared secret' of Gentry 554 is not output at all by any entity, the second intermediate shared secret is output by entity B and the first intermediate shared secret is output by entity A.

Differences between Gentry 554 and Claim 8

Considering in turn the five steps carried out by the third-party computer entity of claim 8:

receiving both data indicative of said first element, and a first product formed by the first party from a first secret and the first element;

The examiner, by equating the 'first element' to **P** and the 'first product' to **aP** (see page 9 of Official Action), implicitly equates the third-party computer entity of claim 1 with entity B, as it is only entity B of Gentry 554 which receives both these quantities.

receiving in respect of the second party both an identifier string, and first, second and third verification parameters;

From above, the 'third-party computer entity' is entity B; the 'second party' must therefore be entity A since Gentry 554 only discloses the entities A and B as having identities from which respective elements are formed (see paragraph [0022]). Entity B in Gentry 554 clearly does receive the identity of entity A since it needs it to compute $\mathbf{P}_A$ when determining the non-interactive shared secret $\mathbf{S}_{AB}$.

The examiner goes on to argue that entity B also receives three parameters **abP**, **b**, and **aP**. However, as already noted, entity B does not receive **abP** but computes it from **aP** and its secret b. Furthermore, entity B does not receive **b** but selects it (see [0033], line 7). Entity B does receive **aP** from entity A.

computing the second element from the identifier string of the second party;

As already noted, the entity B does compute $\mathbf{P}_A$ from the identity string of entity A.

carrying out a first check: p(third verification parameter, computed second element)= p(first element, second verification parameter)

carrying out a second check: p(first element, first verification parameter)= p(first product, second verification parameter)

These limitations are addressed in the Appeal Brief.

Summary

Withdrawal of the rejections and allowance of the claims are respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is electronically filed with the United States Patent and Trademark Office on

18 September 2008
(Date of Transmission)

Lonnie Louie
(Name of Person Transmitting)

/Lonnie Louie/
(Signature)

18 September 2008
(Date)

Respectfully submitted,

/Richard P. Berg 28145/

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile